(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020030035737 A
(43)Date of publication of application: 09.05.2003

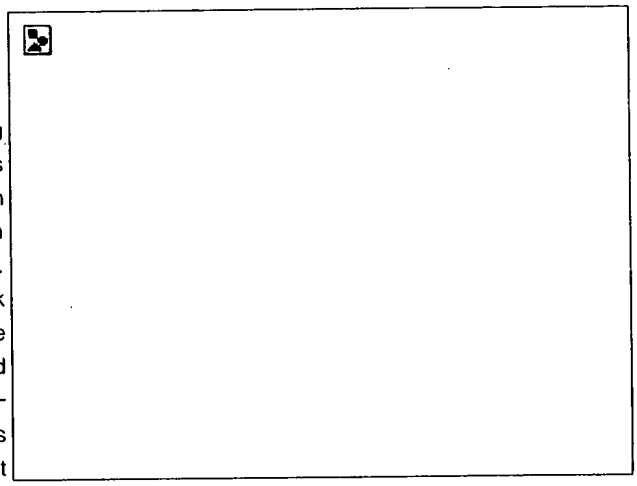
(21)Application number: 1020020003309
(22)Date of filing: 21.01.2002

(71)Applicant: SAMSUNG ELECTRONICS CO., LTD.
(72)Inventor: LEE, HUN JAE
MUN, SANG JAE
PARK, SANG JUN

(51)Int. Cl H04L 9 /22

(54) RANDOM KEY STREAM GENERATING APPARATUS USED IN CIPHER SYSTEM AND METHOD

(57) Abstract:



PURPOSE: A random key stream generating apparatus used in cipher system and method is provided to generate a random key stream, used in a cipher system or a spread spectrum communication system, in a high speed. CONSTITUTION: A parallel shifting linear feedback shift register(PS-LFSR)(110) consists of n store stages for storing n-bit binary data and is divided into k sub-store parts. The sub-store parts store m-bit parallel binary data from previous sub-store parts at the same time and output the stored m-bit parallel binary data according to a system clock. A buffer(120) consists of m store stages so as to simultaneously store and output m-bit parallel binary data from the last sub-store part of the PS-LFSR. M feedback connections(130) receive outputs of the sub-store parts and the buffer corresponding to predetermined original polynomials, perform calculations according to the original polynomials, and output calculation results as respective bits of a ky stream.

Legal Status
Date of request for an examination (20020121)
Notification date of refusal decision (00000000)
Final disposal of an application (registration)
Date of final disposal of an application (20031210)
Patent registration number (1004169710000)
Date of registration (20040117)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2003-0035737
H04L 9/22		(43) 공개일자	2003년05월09일
(21) 출원번호	10-2002-0003309		
(22) 출원일자	2002년01월21일		
(30) 우선권주장	1020010061691 2001년10월06일 대한민국(KR)		

(71) 출원인 삼성전자주식회사
대한민국
442-742
경기도 수원시 팔달구 매탄3동 416번지

(72) 발명자 이훈재
대한민국
706-825
대구광역시수성구범어1동665계림빌라가-401

문상재
대한민국
701-030
대구광역시동구효목동55진로이스타운101-904

박상준
대한민국
137-070
서울특별시서초구서초동1564-6202호

(74) 대리인 이건주

(77) 심사청구 있음

(54) 출원명 암호시스템에 사용하기 위한 랜덤 키스트림 생성 장치 및방법

요약

병렬 이동형 선형피드백 시프트레지스터(PS-LFSR)를 사용하여 랜덤 키스트림을 생성하는 장치 및 방법이 개시되어 있다. 상기 장치의 PS-LFSR은 n개의 저장 스테이지들로 구성되고, k(여기서, k는 n에서 m을 나눈 수보다 큰 최소 정수)개의 서브저장부들로 분할되고, 상기 각 서브저장부들은, 이전의 서브저장부들로부터 입력되는 m비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 m비트의 병렬 이진 데이터들을 시스템 클럭에 따라 출력한다. 버퍼는 상기 시프트 레지스터의 마지막 서브저장부로부터 출력되는 m비트의 병렬 이진 데이터들을 동시에 저장 및 출력하기 위한 m개의 저장 스테이지들로 구성된다. m개의 피드백 컨넥션들은 미리 정해진 원시 다항식에 대응하는 상기 서브저장부들의 출력과 상기 버퍼의 출력을 제공받고 상기 원시 다항식에 따른 연산을 각각 수행하고 연산 결과를 상기 키스트림의 각 비트들로서 출력한다.

대표도

도2

색인어

랜덤 키스트림, 스트림 암호, 선형피드백 시프트레지스터(LFSR)

영세서

도면의 간단한 설명

도 1은 종래 기술에 따른 선형피드백 시프트레지스터를 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도.

도 2는 본 발명의 실시예에 따른 (n, m) 병렬 이동형 선형패드백 시프트레지스터(PS-LFSR)를 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도.

도 3은 본 발명의 실시예에 따른 (40, 8) 선형피드백 시프트레지스터를 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도.

도 4는 본 발명의 실시예에 따른 (39, 8) 선형피드백 시프트레지스터를 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 암호시스템에 관한 것으로, 특히 선형피드백 시프트레지스터(LFSR)를 사용하여 입력 정보의 암호화를 위한 랜덤 키스트림을 생성하는 장치 및 방법에 관한 것이다.

최근 통신망의 급격한 발전과 더불어 처리할 데이터도 텍스트/음성 데이터에서 화상회의나 동영상 자료 등 점차 멀티미디어 자료 형태로 변모해 가고 있다. 이에 따라 통신 시스템에서 사용되는 암호 알고리듬도 고비도, 고속화 및 고신뢰도 설계가 요구되고 있다.

일반적으로 암호 방식은 스트림 암호(stream cipher), 블록 암호(block cipher) 그리고 공개키 암호(public key cipher)로 분류될 수 있다. 상기 블록 암호는 적용 방식에 따라 ECB(Electronic CodeBook) 모드, CFB(Cipher FeedBack) 모드, CBC(Cipher Block Chaining) 모드 및 OFB(Output FeedBack) 모드로 구분된다. 상기 ECB 모드는 블록 크기의 입력에 대하여 비밀키(Secret Key)와 DES(Data Encryption Standard) 함수로부터 블록 출력을 생성하는 방식이다. 상기 CFB 모드는 출력 암호문을 입력에 피드백(feedback)시킨다. 상기 CBC 모드는 송수신 데이터 인증을 위하여 현재 암호문 블록과 다음 번 평문 블록을 배타적논리합(XOR: exclusive-OR) 연산시킨 후 블록 암호에 입력시켜 새로운 출력을 생성하고; 이 출력을 다시 그 다음 번 입력과 XOR시키는 반복 과정으로 최종 인증 값을 얻는 방식이다. 이러한 CBC 모드는 데이터 위조시 최종 인증 값이 바뀌게 되므로 진위 구별이 가능하다. 상기 OFB 모드는 블록 암호 자체를 랜덤 스트림 발생기(random stream generator)로 변경하여 스트림 암호처럼 적용시킨다.

상기 4가지 방식들의 블록 암호는 모두 실제 암호 통신을 하는 실용화 측면에서 채널 에러에 대부분 취약하거나 또 다른 문제점을 안고 있기 때문에 어떤 대책이 요구된다. 구체적으로 말하면, 상기 ECB 모드에서는, 하나의 암호문 블록에서의 하나 또는 그 이상의 비트 에러들은 단지 그 블록의 해독에 영향을 미친다. 상기 CFB 모드에서는, 하나의 암호문 블록에서의 하나의 비트 에러는 그 블록과 다음 블록의 해독에 영향을 미친다. 상기 CBC 모드에서는, 하나의 암호문 블록에서의 하나의 비트 에러는 이후 모든 블록들에 영향을 미친다. 블록 암호의 에러 확산을 줄이기 위하여 도입된 OFB 모드는 입력 피드백 비트 수(이 수는 블록 크기보다 작음)만큼 확산을 줄일 수 있으며, 최상의 경우 1비트를 피드백시켜 근본적으로 확산을 방지할 수 있다. 하지만 1비트 크기의 OFB 모드는 일반 ECB 모드보다는 데이터 처리 속도가 블록 크기 배 감소되기 때문에 오히려 통신망 처리 능력을 떨어뜨린다.

또한, 공개키 암호는 처리 속도가 느리기 때문에 고속 데이터 처리에 부적합할 뿐 아니라 ECB 모드처럼 에러가 블록 전체로 확산되는 단점이 있다. 또한, 스트림 암호는 채널 에러 확산이 없고 안전성(비도 수준) 요소가 몇 가지 측면에서 수학적으로 보장이 되며 고속 처리가 가능한 장점이 있지만, 이 방법 역시 초고속 통신 서비스에 따른 암호 처리를 원활하게 할 수 있을지는 의문이다.

한편, 스트림 암호를 구현시에 많이 사용되는 소자로 선형피드백 시프트레지스터(LFSR: Linear Feedback Shift Register)와 비선형 결합함수형태의 논리조합회로, 전가산기(full adder), 멀티플렉서(multiplexer) 등을 들 수 있다. 특히 LFSR은 크기의 다양성 뿐만 아니라 키 수열의 주기라는 비도 요소를 결정짓기 때문에 암호시스템에서는 거의 필수적으로 사용되고 있는 소자이다. 상기 LFSR은 도 1에 도시된 바와 같이 외부에서 입력되는 시스템 클럭에 맞추어 동기적으로 1비트씩 이동시키면서 이진 키 스트림(key stream)을 발생한다. 상기 발생된 키 스트림은 암호화 결합기(Encryption Combiner)(도시하지 않음)로 제공되어 평문(plain text)을 암호문(Cipher Text)으로 변환하는데 이용된다. 이때 상기 키 스트림의 발생 속도는 시스템 클럭과 내부 회로의 지연시간에 의해서 결정된다.

전술한 도 1에 도시된 바와 같은 LFSR은 의사잡음(Pseudo Noise) 부호의 생성이나 암호화를 위한 처리에서 필수적으로 사용되는 소자이다. 특히 암호화되어야 할 대상이 멀티미디어 서비스를 위한 데이터로 점차적으로 변화되고 있는 추세에 비추어볼 때 고속의 LFSR 처리가 필요하다. 그러나 종래 기술에 따른 LFSR 구조는 한 시스템 클럭에 한 비트씩의 이동만을 가능하게 하므로, 고속의 LFSR 처리에는 적합하지 않은 구조라고 말할 수 있다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명의 목적은 암호시스템 혹은 확산 스펙트럼 통신시스템에서 사용하기 위한 랜덤 키스트림을 고속으로 생성하는 장치 및 방법을 제공함에 있다.

본 발명의 다른 목적은 고속으로 동작하는 LFSR을 구현하여 실시간 처리 및 대용량 처리, 많은 계산량을 요구하는 암호화 처리시 시간의 지연을 줄일 수 있도록 하는 장치 및 방법을 제공함에 있다.

본 발명의 또 다른 목적은 암호시스템 혹은 확산 스펙트럼 통신시스템에서 통신 채널을 통한 에러 확산을 제거하기 위한 장치 및 방법을 제공함에 있다.

이러한 목적들을 달성하기 위한 본 발명은 하나의 시스템 클럭내에서 m비트 이동이 가능하고, 최종 출력이 m비트 발생될 수 있도록 하는 병렬 이동형 선형피드백 시프트 레지스터(PS-LFSR)를 포함하는 랜덤 키스트림 생성 장치를 제안한다. 상기 장치의 PS-LFSR은 n비트의 이진 데이터를 저장하기 위한 n개의 저장 스테이지들로 구성되고, k(여기서, k는 n에서 m을 나눈 수보다 큰 최소 정수)개의 서브저장부들로 분할되고, 상기 각 서브저장부들은, 이전의 서브저장부들로부터 입력되는 m비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 m비트의 병렬 이진 데이터들을 시스템 클럭에 따라 출력한다. 버퍼는 상기 시프트 레지스터의 마지막 서브저장부로부터 출력되는 m비트의 병렬 이진 데이터들을 동시에 저장 및 출력하기 위한 m개의 저장 스테이지들로 구성된다. m개의 피드백 컨넥션들은 미리 정해진 원시 다항식에 대응하는 상기 서브저장부들의 출력과 상기 버퍼의 출력을 제공받고 상기 원시 다항식에 따른 연산을 각각 수행하고 연산 결과를 상기 키스트림의 각 비트들로서 출력한다.

발명의 구성 및 작용

이하 본 발명의 바람직한 실시예의 상세한 설명이 첨부된 도면들을 참조하여 설명될 것이다. 도면들 중 참조번호들 및 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 참조번호들 및 부호들로 나타내고 있음에 유의해야 한다. 하기에서 본 발명을 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

하기에서 본 발명은 암호시스템의 초고속화와 통신 채널을 통한 에러 확산을 제거할 수 있는 암호시스템의 설계라는 두 가지 목적들 하에서, 스트림 암호와 블록 암호의 장점들을 혼합시킨 병렬 이동형 선형피드백 시프트레지스터(PS-LFSR: Parallel Shifting Linear Feedback Shift Register)와 그를 포함하여 랜덤 키스트림을 생성하는 장치를 제안한다. 즉, 본 발명의 실시예는 스트림 암호의 비도 수준과 에러 확산 방지 기능을 유지하면서 블록 암호의 m비트 병렬 처리 기능을 혼합시켜 고속 암호화 처리를 가능하게 한다. 스트림 암호에서 LFSR은 한 클럭에 1비트씩 이동되는데, 이를 개선한 본 발명은 한 클럭에 m비트 이동이 가능하다. 또한 본 발명은 1비트씩 처리되는 비선형 결합함수의 단점을 보완하여 블록 암호처럼 동시에 여러 비트의 출력이 될 수 있도록 하는 m비트 병렬 비선형 결합함수의 일반형을 제안한다.

도 2는 본 발명의 실시예에 따른 (n, m) PS-LFSR을 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도이다.

상기 도 2를 참조하면, 키스트림 생성 장치는 m비트의 랜덤 키스트림을 생성하기 위한 것으로, PS-LFSR 110, 버퍼 120 및 피드백 컨넥션부 130을 포함한다. 상기 PS-LFSR 110은 n비트의 이진 데이터(binary data)를 저장하기 위한 n개의 저장 스테이지(storage stage)들로 구성된다. 상기 PS-LFSR 110은 도 1에 도시된 종래 기술에 따른 LFSR 10과 동일하게 n개의 저장 스테이지들로 구성된다. 그러나 상기 PS-LFSR 110을 구성하는 n개의 저장 스테이지들은 미리 설정된 수(k)만큼의 서브저장부들로 분할되고, 분할된 서브저장부들 각각은 병렬로 배열되는 m개의 저장 스테이지들로 구성되는 것을 특징으로 한다. 이러한 구성은 시스템 클럭의 한 주기내에서 m비트의 이진 데이터를 병렬로 이동, 즉 동시에 저장 및 출력할 수 있도록 한다. 여기서, 상기 설정된 수 k는 n과 m이 주어진다고 가정했을 때, k는 n에서 m을 나눈 수보다 큰 최소 정수로서 결정된다. 일 예로, n=400이고 m=8인 경우, k는 5로서 결정된다. 이때 상기 서브저장부들은 동일한 수(m)의 저장 스테이지들로 구성된다. 다른 예로, n=39이고 m=8인 경우, k는 39에서 8을 나눈 수인 4.875보다 큰 최소 정수 5로서 결정된다. 이때 상기 서브저장부들중의 적어도 한 서브저장부는 나머지 서브저장부들과 상이한 수의 저장 스테이지들로 구성된다. 이러한 예들에 따른 키스트림 생성 장치는 후술될 도 3 및 도 4에 도시되어 있다. 상기 키스트림 생성 장치는 소프트웨어 혹은 하드웨어로 구현될 수도 있으며, 스트림 암호를 사용하는 통신시스템의 키스트림 발생기(keystream generator)에 사용될 수 있다. 본 발명의 실시예에서는 상기 키스트림 생성 장치가 스트림 암호를 사용하는 통신시스템에서의 키스트림 발생기로서 사용되는 경우로 설명될 것이지만, 확산 스펙트럼(spread spectrum) 통신시스템의 의사잡음 발생기(pseudo-noise generator) 등에 사용될 수 있다는 사실에 유의하여야 한다.

다시 도 2를 참조하면, 상기 PS-LFSR 110은 k개의 서브저장부들 111~115로 분할된다. 서브저장부 111은 상기 n개의 저장 스테이지들중 첫 번째 m개의 저장 스테이지들(n-1, n-2, n-3, n-4, n-5, n-6, ····, n-m)로 구성된다. 서브저장부 113은 상기 n개의 저장 스테이지들중 m개의 저장 스테이지들(3m-1, ····, 2m+5, 2m+4, 2m+3, 2m+2, 2m+1, 2m)로 구성된다. 서브저장부 114는 상기 n개의 저장 스테이지들중 m개의 저장 스테이지들(2m-1, ····, m+5, m+4, m+3, m+2, m+1, m)로 구성된다. 서브저장부 115는 상기 n개의 저장 스테이지들중 마지막 번째 m개의 저장 스테이지들(m-1, ····, 5, 4, 3, 2, 1, 0)로 구성된다. 상기 서브저장부들 111~115 각각을 구성하는 저장 스테이지들은 병렬로 배열된다. 이에 따라 상기 각 서브저장부들 111~115는 이전의 서브저장부들로부터 입력되는 m비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 m비트의 병렬 이진 데이터들을 시스템 클럭(System Clock)에 따라 출력한다.

버퍼 120은 상기 PS-LFSR 110의 마지막 서브저장부 115로부터 출력되는 m비트의 병렬 이진 데이터들을 동시에 저장 및 출력하기 위한 m개의 저장 스테이지들(-m, -(m-1), ····, -5, -4, -3, -2, -1)로 구성된다. 이때 상기 버퍼 120의 첫 번째 저장 스테이지(-m)는 사용되지 않는다. 왜냐하면, 상기 버퍼 120의 첫 번째 저장 스테이지(-m)에 저장되는 값은 이후에 설명될 피드백 컨넥션부 130에서 사용되지 않기 때문이다. 즉, 상기 버퍼 120은 (m-1)개의 저장 스테이지들로 구성되어도 무방하다. 이러한 버퍼 120은 시스템 클럭의 다음 주기에서 사용될 저장 스테이지들의 값들을 저장하기 위한 것이다.

피드백 컨넥션부(Feedback Connection Unit) 130은 m개의 피드백 컨넥션들 131~133으로 구성된다. 상기 피드백 컨넥션들 131~133은 각각 키스트림 생성을 위해 미리 정해진 원시 다항식(primitive polynomial)에 따른 연산을 행하기 위한 것으로, 각각 정해진 원시 다항식에 대응하는 상기 서브저장부들 111~115의 출력과 상기 버퍼 120의 출력을 제공받고, 상기 원시 다항식에 따른 연산을 각각 수행하고 해당하는 연산 결과를 상기 키스트림의 각 비트들로서 출력한다. 상기 피드백 컨넥션들 131~133은 복수개의 배타적논리합(XOR: Exclusive OR) 연산기들로서 구현될 수 있다. 상기 피드백 컨넥션 131에 대해 임의의 원시 다항식이 정해졌을 때, 피드백 컨넥션 132는 상기 피드백 컨넥션 131에 대해 정해진 원시 다항식을 1비트 왼쪽으로 시프트한 결과에 따른 원시 다항식에 따른 연산을 수행하고, 피드백 컨넥션 133은 상기 피드백 컨넥션 131에 대해 정해진 원시 다항식을 m비트 왼쪽으로 시프트한 결과에 따른 원시 다항식에 따른 연산을 수행한다. 그러므로, 상기 피드백 컨넥션 131에 0번째, 1번째, 2번째, ····, (n-1)번째 저장 스테이지들에 저장된 값들이 제공된다고 가정했을 때, 상기 피드백 컨넥션 132은 (-1)번째, 0번째, 1번째, ····, (n-2)번째 저장 스테이지들에 저장된 값들을 입력하여 해당하는 연산을 수행하고, 상기 피드백 컨넥션 133은 -(m-1)번째, -(m-2)번째, -(m-3)번째, ····, (n-m+1)번째 저장 스테이지들에 저장된 값들을 입력하여 해당하는 연산을 수행한다. 상기 피드백 컨넥션 131은 1번째 피드백값을 출력하고, 상기 피드백 컨넥션 132는 2번째 피드백값을 출력하고, 상기 피드백 컨넥션 133은 m번째 피드백값을 출력한다. 상기 피드백 컨넥션들 131~133으로부터 출력되는 피드백 값들은 상기 PS-LFSR 110의 서브저장부 111의 해당하는 저장 스테이지들로 입력되어 이후의 키스트림 생성에 사용된다. 상기 피드백 컨넥션 131로부터 출력되는 1번째 피드백값(feedback 1)은 서브저장부 111의 (n-m) 저장 스테이지로 입력되고, 상기 피드백 컨넥션 132로부터 출력되는 2번째 피드백값(feedback 2)은 서브저장부 111의 (n-m-1) 저장 스테이지로 입력되고, 상기 피드백 컨넥션 133으로부터 출력되는 m번째 피드백값은 서브저장부 111의 (n-1) 저장 스테이지로 입력된다. 모든 피드백 컨넥션들 131~133에 의해 연산된 결과에 따른 피드백 값들이 출력되는 경우에는 이 피드백 값들은 암호화 처리를 위한 m비트의 키스트림으로서 생성된다.

상기 도 2에 도시된 랜덤 키스트림 생성 장치이 m비트의 랜덤 키스트림을 생성하는 동작은 다음과 같이 수행된다.

(과정 1) n비트의 이진 데이터를 저장하기 위한 n개의 저장 스테이지들로 구성되는 PS-LFSR 110은 k(여기서, k는 n에서 m을 나눈 수보다 큰 최소 정수)개의 서브저장부들 111~115로 분할된다.

(과정 2) 상기 각 서브저장부들 111~115은 이전의 서브저장부들로부터 입력되는 m비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 m비트의 병렬 이진 데이터들을 시스템 클럭에 따라 출력한다.

(과정 3) 버퍼 120은 상기 PS-LFSR 110의 마지막 서브저장부 115로부터 출력되는 m비트의 병렬 이진 데이터들을 버퍼링한다.

(과정 4) 피드백 컨넥션 131은 미리 정해진 원시 다항식에 대응하는 상기 서브저장부들 111~115의 출력을 제공받고 상기 원시 다항식에 따른 연산을 수행하여 최초 피드백 결과값(feedback 1)을 출력한다.

(과정 5) 상기 원시 다항식을 1비트 왼쪽으로 시프트시키면서 (m-1)개의 원시 다항식들을 생성한다. 이렇게 생성된 (m-1)개의 원시 다항식들은 (m-1)개의 피드백 컨넥션들 132~133에 사용하기 위한 원시 다항식들이다.

(과정 6) 피드백 컨넥션들 132~133은 각각 상기 (m-1)개의 원시 다항식들에

대응하는 상기 서브저장부들 111~115의 출력과 상기 버퍼 120에 버퍼링된 값을 제공받고 상기 (m-1)개의 원시 다항식들 각각에 따른 연산을 수행하여 (m-1)개의 피드백 결과값들(feedback 2 ~feedback m)을 출력한다.

(과정 7) 상기 m개의 피드백 결과값들은 m비트의 키스트링의 각 비트들로서 출력된다.

전술한 바와 같이, 본 발명의 실시예에 따른 PS-LFSR을 포함하는 랜덤 키스트림 생성 장치는 모든 비트가 m비트 단위의 병렬이동(parallel shifting)을 가능하도록 하기 위하여 병렬 경로가 구성되어 있다. 피드백 컨넥션(탭)에서도 m묶음의 XOR 조합 연산을 행하고, 그 결과는 맨 오른쪽 배열 레지스터 111에 동시에 제공된다. 다음의 시스템 클럭(시정)에서는 맨 오른쪽 배열에서 각각 왼쪽 배열로 m비트 블록 단위로 이동되고, 계속해서 왼쪽으로 블록 크기(m) 단위만큼 병렬 이동된다. 결국 이러한 랜덤 키스트램 생성 장치는 한 클럭에 m비트 이동 후 m비트(또는 그 이하)출력을 동시 생성하는 발생기로서, 긴 주기에서의 출력 스트림은 단 한번만 사용되므로 랜덤 특성, 주기 등 비도 특성이 도 1에 도시된 바와 같은 일반적인 LFSR과 동일함을 알 수 있다. 또한 비트 단위의 출력을 발생하는 LFSR과 비교할 때 PS-LFSR은 암호화 처리속도가 m배 빨라지며, 고속화에 따른 하드웨어 복잡도는 다소 증가될 수 있지만 최근의 집적회로 기술 발전으로 큰 문제가 되지 않을 것이다.

도 3은 본 발명의 실시예에 따른 (40, 8) PS-LFSR을 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도이다. 이 실시예에 따른 랜덤 키스트림 생성 장치는 (n,m) PS-LFSR의 설계 예로서 n = km(k는 정수)가 되는 (40,8) PS-LFSR을 포함한다.

상기 도 3을 참조하면, 키스트림 생성 장치는 8비트의 랜덤 키스트림을 생성하기 위한 것으로, PS-LFSR 210, 버퍼 220 및 피드백 컨넥션부 230을 포함한다. 상기 PS-LFSR 210은 40비트의 이진 데이터를 저장하기 위한 40개의 저장 스테이지(storage stage)들로 구성된다. 상기 PS-LFSR 210을 구성하는 40개의 저장 스테이지들은 미리 설정된 수(k=5)만큼의 서브저장부들로 분할되고, 분할된 서브저장부들 각각은 병렬로 배열되는 8개의 저장 스테이지들로 구성되는 것을 특징으로 한다. 이러한 구성은 시스템 클럭의 한 주기내에서 8비트의 이진 데이터를 병렬로 이동, 즉 동시에 저장 및 출력할 수 있도록 한다.

상기 PS-LFSR 210은 5개의 서브저장부들 211~215로 분할된다. 이때 서브저장부들 211~215 각각은 동일한 수(m=8)의 저장 스테이지들로 구성된다. 서브저장부 211은 상기 40개의 저장 스테이지들중 첫 번째 8개의 저장 스테이지들(39~32)로 구성된다. 서브저장부 212는 상기 40개의 저장 스테이지들중 8개의 저장 스테이지들(31~24)로 구성된다. 서브저장부 213은 상기 40개의 저장 스테이지들중 8개의 저장 스테이지들(23~16)로 구성된다. 서브저장부 214는 상기 40개의 저장 스테이지들중 8개의 저장 스테이지들(15~8)로 구성된다. 서브저장부 215는 상기 40개의 저장 스테이지들중 마지막 번째 8개의 저장 스테이지들(7~0)로 구성된다. 상기 서브저장부들 211~215 각각을 구성하는 저장 스테이지들은 병렬로 배열된다. 이에 따라 상기 각 서브저장부들 211~215는 이전의 서브저장부들로부터 입력되는 8비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 8비트의 병렬 이진 데이터들을 시스템 클럭(System Clock)에 따라 출력한다.

버퍼 220은 상기 PS-LFSR 210의 마지막 서브저장부 215로부터 출력되는 8비트의 병렬 이진 데이터들을 동시에 저장 및 출력하기 위한 8개의 저장 스테이지들(-8,-7,-6,-5,-4,-3,-2,-1)로 구성된다. 이때 상기 버퍼 220의 첫 번째 저장 스테이지(-8)는 사용되지 않는다. 즉, 상기 버퍼 220은 7개의 저장 스테이지들로 구성되어도 무방하다. 이러한 버퍼 220은 시스템 클럭의 다음 주기에서 사용될 각 저장 스테이지들의 값들을 저장하기 위한 것이다.

피드백 컨넥션부 230은 8개의 피드백 컨넥션들 231~233으로 구성된다. 상기 피드백 컨넥션들 231~233은 각각 키스트림 생성을 위해 미리 정해진 원시 다항식(primitive polynomial)에 따른 연산을 행하기 위한 것으로, 각각 정해진 원시 다항식에 대응하는 상기 서브저장부들 211~215의 출력과 상기 버퍼 220의 출력을 제공받고, 상기 원시 다항식에 따른 연산을 각각 수행하고 해당하는 연산 결과를 상기 키스트림의 각 비트들로서 출력한다. 상기 피드백 컨넥션 231에 대해 임의의 원시 다항식이 정해졌을 때, 피드백 컨넥션 232는 상기 피드백 컨넥션 231에 대해 정해진 원시 다항식을 1비트 왼쪽으로 시프트한 결과에 따른 원시 다항식에 따른 연산을 수행하고, 피드백 컨넥션 233은 상기 피드백 컨넥션 231에 대해 정해진 원시 다항식을 8비트 왼쪽으로 시프트한 결과에 따른 원시 다항식에 따른 연산을 수행한다. 그러므로, 상기 피드백 컨넥션 231에 0번째, 1번째, 2번째, ···· , 35번째 저장 스테이지들에 저장된 값들이 제공된다고 가정했을 때, 상기 피드백 컨넥션 232는 (-1)번째, 0번째, 1번째, ···· , 34번째 저장 스테이지들에 저장된 값들을 입력하여 해당하는 연산을 수행하고, 상기 피드백 컨넥션 233은 -7번째, -6번째, -5번째, ···· , 28번째 저장 스테이지들에 저장된 값들을 입력하여 해당하는 연산을 수행한다. 즉, 상기 피드백 컨넥션 231에 대해 정해진 원시 다항식이 s(40+t)=s(35+t)^s(2+t)^s(1+t)^s(t)(여기서, ^는 배타적 논리합(XOR: eXclusive OR) 연산을 나타냄.)라고 가정할 때, 상기 피드백 컨넥션 232는 원시 다항식 s(39+t)=s(34+t)^s(1+t)^s(t)^s(-1+t)에 따른 연산을 수행하고, 상기 피드백 컨넥션 233은 원시 다항식 s(33+t)=s(28+t)^s(-5+t)^s(-6+t)^s(-7+t)에 따른 연산을 수행한다.

상기 피드백 컨넥션 231은 1번째 피드백값을 출력하고, 상기 피드백 컨넥션 232는 2번째 피드백값을 출력하고, 상기 피드백 컨넥션 233은 8번째 피드백값을 출력한다. 상기 피드백 컨넥션들 231~233으로부터 출력되는 피드백 값들은 상기 PS-LFSR 210의 서브저장부 211의 해당하는 저장 스테이지들로 입력되어 이후의 키스트림 생성에 사용된다. 상기 피드백 컨넥션 231로부터 출력되는 1번째 피드백값(feedback 1)은 서브저장부 211의 32 저장 스테이지로 입력되고, 상기 피드백 컨넥션 232로부터 출력되는 2번째 피드백값(feedback 2)은 서브저장부 211의 33 저장 스테이지로 입력되고, 상기 피드백 컨넥션 233으로부터 출력되는 8번째 피드백값은 서브저장부 211의 39 저장 스테이지로 입력된다. 모든 피드백 컨넥션들 231~233에 의해 연산된 결과에 따른 피드백 값들이 출력되는 경우에는 이 피드백 값들은 암호화 처리를 위한 8비트의 키스트림으로서 생성된다.

도 4는 본 발명의 실시예에 따른 (39, 8) PS-LFSR을 사용하여 랜덤 키스트림을 생성하는 장치의 블록 구성도이다. 이 실시예에 따른 랜덤 키스트림 생성 장치는 (n,m) PS-LFSR의 설계 예로서 n ≠km(k는 정수)인 (39,8) PS-LFSR을 포함한다.

상기 도 4를 참조하면, 키스트림 생성 장치는 8비트의 랜덤 키스트림을 생성하기 위한 것으로, PS-LFSR 310, 버퍼 320 및 피드백 컨넥션부 330을 포함한다. 상기 PS-LFSR 310은 39비트의 이진 데이터를 저장하기 위한 39개의 저장 스테이지(storage stage)들로 구성된다. 상기 PS-LFSR 310을 구성하는 39개의 저장 스테이지들은 미리 설정된 수(k=5)만큼의 서브저장부들로 분할된다.

상기 PS-LFSR 310은 5개의 서브저장부들 311~315로 분할된다. 이때 상기 서브저장부들중의 적어도 한 서브저장부는 나머지 서브저장부들과 상이한 수의 저장 스테이지들로 구성된다. 예를 들어, 서브저장부 311은 7개의 저장 스테이지들로 구성되고, 나머지 서브저장부들 312~315는 8개의 저장 스테이지들로 구성된다. 상기 PS-LFSR 310의 첫 번째 서브저장부 311은 7개의 저장스테이지들로 구성되고, 나머지 4개의 서브저장부들 312~315는 8개의 저장스테이지들로 구성된다. 서브저장부 311은 상기 39개의 저장 스테이지들중 첫 번째 7개의 저장 스테이지들(38~32)로 구성된다. 서브저장부 312는 상기 39개의 저장 스테이지들중 8개의 저장 스테이지들(31~24)로 구성된다. 서브저장부 313은 상기 39개의 저장 스테이지들중 8개의 저장 스테이지들(23~16)로 구성된다. 서브저장부 314는 상기 39개의 저장 스테이지들중 8개의 저장 스테이지들(15~8)로 구성된다. 서브저장부 315는 상기 39개의 저장 스테이지들중 마지막 번째 8개의 저장 스테이지들(7~0)로 구성된다. 상기 서브저장부들 311~315 각각을 구성하는 저장 스테이지들은 병렬로 배열된다. 이에 따라 상기 각 서브저장부들 311~315는 이전의 서브저장부들로부터 입력되는 7비트 혹은 8비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 7비트 혹은 8비트의 병렬 이진 데이터들을 시스템 클럭(System Clock)에 따라 출력한다.

버퍼 320은 상기 PS-LFSR 310의 마지막 서브저장부 315로부터 출력되는 8비트의 병렬 이진 데이터들을 동시에 저장 및 출력하기 위한 8개의 저장 스테이지들(-8,-7,-6,-5,-4,-3,-2,-1)로 구성된다. 이때 상기 버퍼 320의 첫 번째 저장 스테이지(-8)는 사용되지 않는다. 즉, 상기 버퍼 320은 7개의 저장 스테이지들로 구성되는 버퍼이다. 이러한 버퍼 320은 시스템 클럭의 다음 주기에서 사용될 각 저장 스테이지들의 값들을 저장하기 위한 것이다.

피드백 컨넥션부 330은 8개의 피드백 컨넥션들 331~333으로 구성된다. 상기 피드백 컨넥션들 331~333은 각각 키스트림 생성을 위해 미리 정해진 원시 다항식(primitive polynomial)에 따른 연산을 행하기 위한 것으로, 각각 정해진 원시 다항식에 대응하는 상기 서브저장부들 311~315의 출력과 상기 버퍼 320의 출력을 제공받고, 상기 원시 다항식에 따른 연산을 각각 수행하고 해당하는 연산 결과를 상기 키스트림의 각 비트들로서 출력한다. 상기 피드백 컨넥션 331에 대해 임의의 원시 다항식이 정해졌을 때, 피드백 컨넥션 332는 상기 피드백 컨넥션 331에 대해 정해진 원시 다항식을 1비트 왼쪽으로 시프트한 결과에 따른 원시 다항식에 따른 연산을 수행하고, 피드백 컨넥션 333은 상기 피드백 컨넥션 331에 대해 정해진 원시 다항식을 8비트 왼쪽으로 시프트한 결과에 따른 원시 다항식에 따른 연산을 수행한다. 그러므로, 상기 피드백 컨넥션 331에 0번째, 1번째, 2번째, ···· , 38번째 저장 스테이지들에 저장된 값들이 제공된다고 가정했을 때, 상기 피드백 컨넥션 332는 (-1)번째, 0번째, 1번째, ···· , 37번째 저장 스테이지들에 저장된 값들을 입력하여 해당하는 연산을 수행하고, 상기 피드백 컨넥션 333은 -7번째, -6번째, -5번째, ···· , 30번째 저장 스테이지들에 저장된 값들을 입력하여 해당하는 연산을 수행한다. 즉, 상기 피드백 컨넥션 331에 대해 정해진 원시 다항식이

$$p(x)=x^{39}+x^{37}+x^{25}+x^{24}+x^{22}+x^{8}+x^{6}+x^{4}+1$$

라고 가정할 때, 상기 피드백 컨넥션 332는 원시 다항식

$$p(x)=x^{38}+x^{36}+x^{24}+x^{23}+x^{21}+x^{7}+x^{5}+x^{3}+x^{-1}$$

에 따른 연산을 수행하고, 상기 피드백 컨넥션 333은 원시 다항식

$$p(x)=x^{32}+x^{30}+x^{18}+x^{17}+x^{15}+x^{1}+x^{-1}+x^{-3}+x^{-6}$$

에 따른 연산을 수행한다.

상기 피드백 컨넥션 331은 1번째 피드백값을 출력하고, 상기 피드백 컨넥션 332는 2번째 피드백값을 출력하고, 상기 피드백 컨넥션 333은 8번째 피드백값을 출력한다. 상기 피드백 컨넥션들 331~333으로부터 출력되는 피드백 값들은 상기 PS-LFSR 310의 서브저장부 311의 해당하는 저장 스테이지들로 입력되어 이후의 키스트림 생성에 사용된다. 상기 피드백 컨넥션 331로부터 출력되는 1번째 피드백값(feedback 1)은 서브저장부 312의 31 저장 스테이지로 입력되고, 상기 피드백 컨넥션 332로부터 출력되는 2번째 피드백값(feedback 2)은 서브저장부 311의 32 저장 스테이지로 입력되고, 상기 피드백 컨넥션 333으로부터 출력되는 8번째 피드백값은 서브저장부 311의 38 저장 스테이지로 입력된다. 모든 피드백 컨넥션들 331~333에 의해 연산된 결과에 따른 피드백 값들이 출력되는 경우에는 이 피드백 값들은 암호화 처리를 위한 8비트의 키스트림으로서 생성된다.

한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 예를 들어, 본 발명의 구체적인 실시 예에서는 랜덤 키스트림 생성 장치가 스트림 암호의 키스트림 발생기로서 사용되는 예로서 설명되었으나, 이러한 랜덤 키스트림 생성 장치는 확산 스펙트럼 통신시스템의 의사잡음 발생기로서도 동일하게 사용될 수 있을 것이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 아니되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

발명의 효과

상술한 바와 같이 본 발명은 고속으로 동작하는 LFSR을 통하여 실시간 처리, 대용량 처리 및 많은 계산량을 요구하는 암호화 처리에서 시간의 지연을 획기적으로 줄일 수 있도록 하는 이점이 있다.

(57) 청구의 범위

청구항 1.

암호시스템에 사용하기 위한 m비트의 랜덤 키스트림을 생성하는 장치에 있어서,

n비트의 이진 데이터를 저장하기 위한 n개의 저장 스테이지들로 구성되고, k(여기서, k는 n에서 m을 나눈 수보다 큰 최소 정수)개의 서브저장부들로 분할되고, 상기 각 서브저장부들은, 이전의 서브저장부들로부터 입력되는 m비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 m비트의 병렬 이진 데이터들을 시스템 클럭에 따라 출력하는 병렬 이동형 선형 피드백 시프트 레지스터(PS-LFSR)와,

상기 시프트 레지스터의 마지막 서브저장부로부터 출력되는 m비트의 병렬 이진 데이터들을 동시에 저장 및 출력하기 위한 m개의 저장 스테이지들로 구성되는 버퍼와,

미리 정해진 원시 다항식에 대응하는 상기 서브저장부들의 출력과 상기 버퍼의 출력을 제공받고 상기 원시 다항식에 따른 연산을 각각 수행하고 연산 결과를 상기 키스트림의 각 비트들로서 출력하는 m개의 피드백 컨넥션들을 포함함을 특징으로 하는 상기 장치.

청구항 2.

제1항에 있어서, 상기 버퍼의 1번째 비트는 사용되지 않음을 특징으로 하는 상기 장치.

청구항 3.
제1항에 있어서, 상기 서브저장부들은 동일한 수의 저장 스테이지들로 구성됨을 특징으로 하는 상기 장치.

청구항 4.
제1항에 있어서, 상기 서브저장부들중의 적어도 한 서브저장부는 나머지 서브저장부들과 상이한 수의 저장 스테이지들로 구성됨을 특징으로 하는 상기 장치.

청구항 5.
암호시스템에 사용하기 위한 m비트의 랜덤 키스트림을 생성하는 방법에 있어서,

n비트의 이진 데이터를 저장하기 위한 n개의 저장 스테이지들로 구성되는 선형 피드백 시프트 레지스터(PS-LFSR)를 k(여기서, k는 n에서 m을 나눈 수보다 큰 최소 정수)개의 서브저장부들로 분할하는 과정과,

상기 각 서브저장부들에서 이전의 서브저장부들로부터 입력되는 m비트의 병렬 이진 데이터들을 동시에 저장하고 저장된 m비트의 병렬 이진 데이터들을 시스템 클럭에 따라 출력하는 과정과,

상기 시프트 레지스터의 마지막 서브저장부로부터 출력되는 m비트의 병렬 이진 데이터들을 버퍼를 통해 버퍼링하는 과정과,

미리 정해진 원시 다항식에 대응하는 상기 서브저장부들의 출력을 제공받고 상기 원시 다항식에 따른 연산을 수행하여 최초 피드백 결과값을 출력하는 과정과,

상기 원시 다항식을 1비트 왼쪽으로 시프트시키면서 (m-1)개의 원시 다항식들을 생성하는 과정과,

상기 (m-1)개의 원시 다항식들에 대응하는 상기 서브저장부들의 출력과 상기 버퍼에 버퍼링된 값을 제공받고 상기 (m-1)개의 원시 다항식들 각각에 따른 연산을 수행하여 (m-1)개의 피드백 결과값들을 출력하는 과정과,

상기 m개의 피드백 결과값들을 상기 키스트림의 각 비트들로서 출력하는 과정을 포함함을 특징으로 하는 상기 방법.

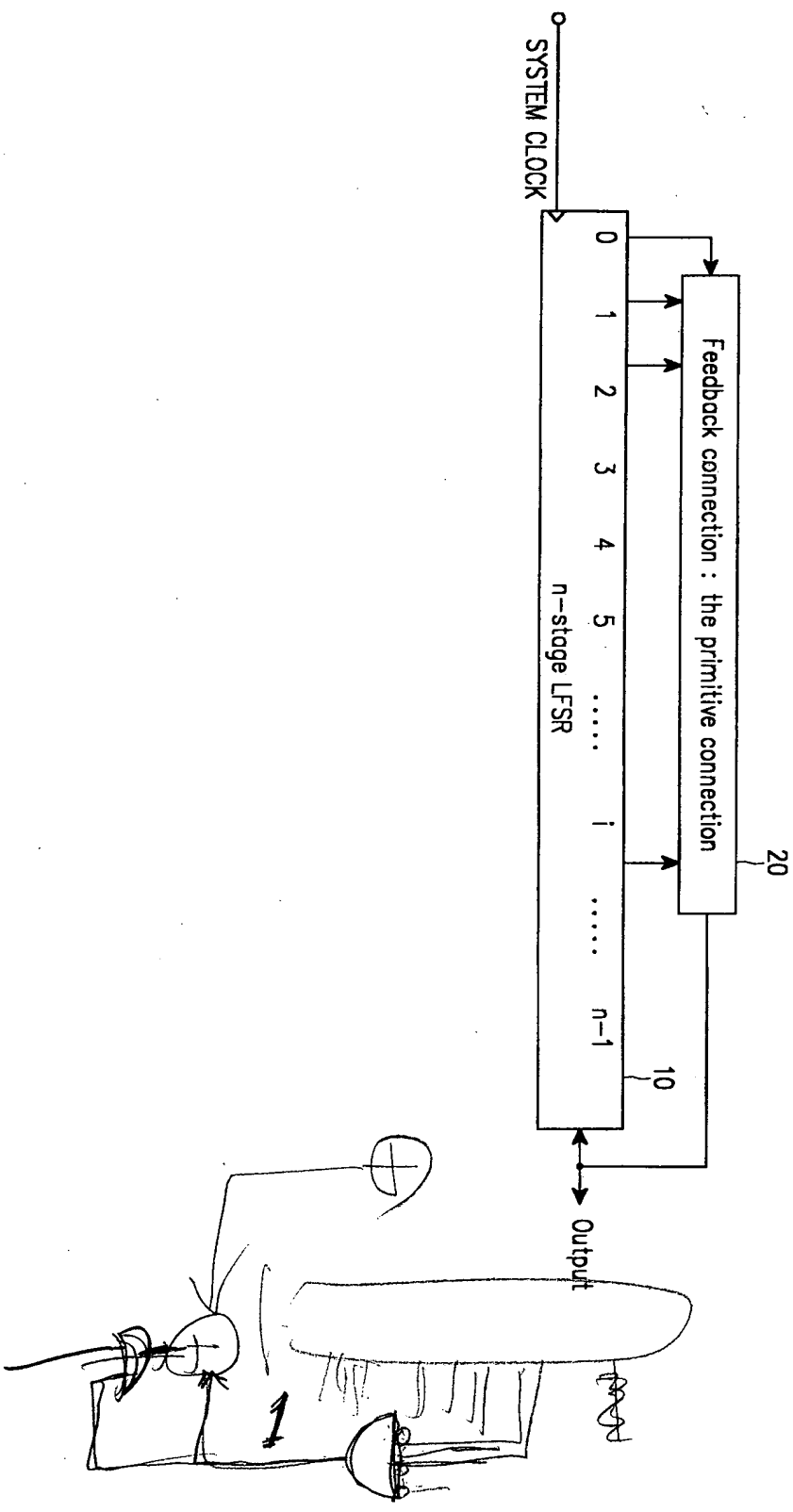
청구항 6.
제5항에 있어서, 상기 버퍼의 1번째 비트는 사용되지 않음을 특징으로 하는 상기 방법.

청구항 7.
제5항에 있어서, 상기 서브저장부들은 동일한 수의 저장 스테이지들로 구성됨을 특징으로 하는 상기 방법.

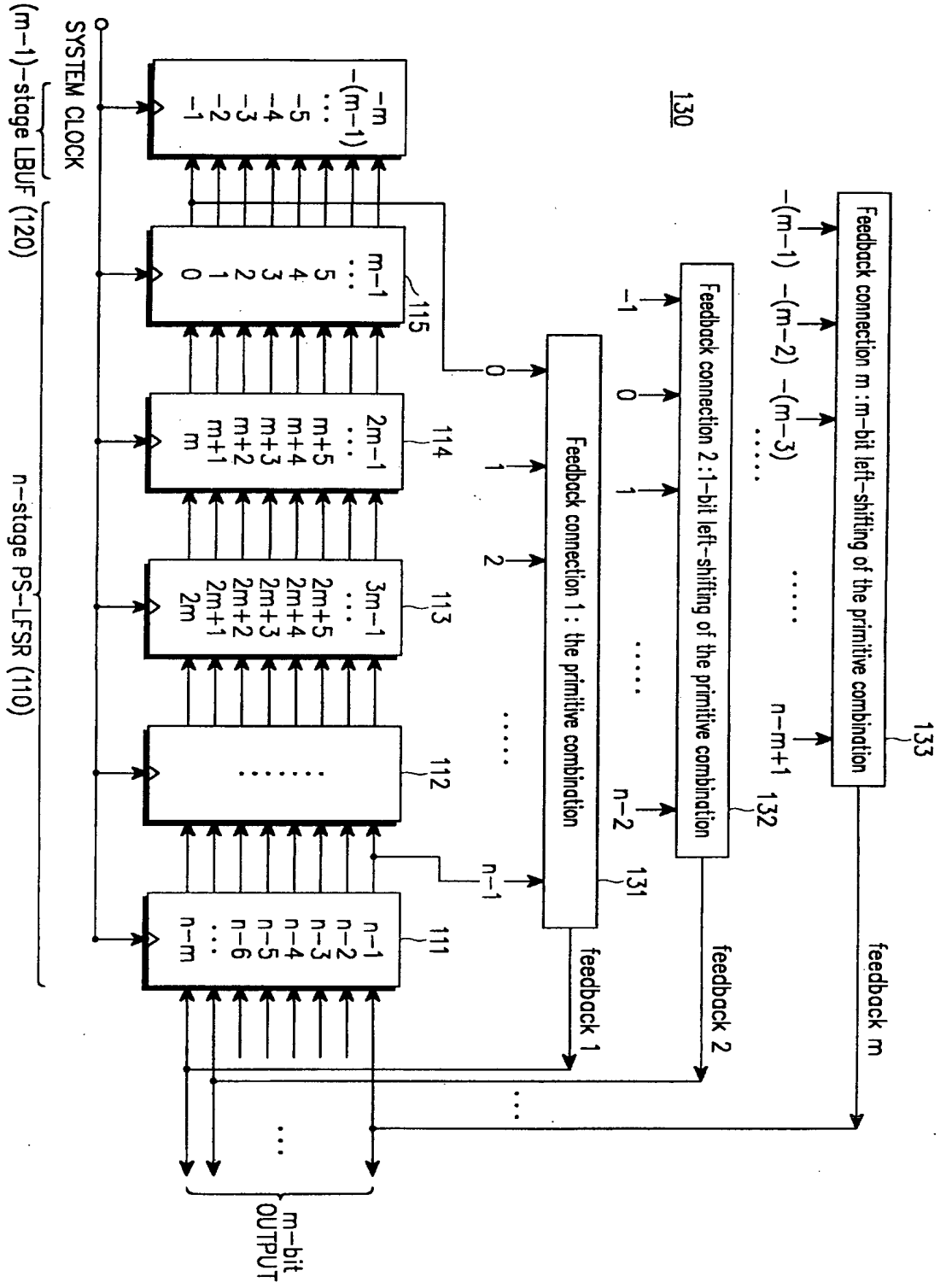
청구항 8.
제5항에 있어서, 상기 서브저장부들중의 적어도 한 서브저장부는 나머지 서브저장부들과 상이한 수의 저장 스테이지들로 구성됨을 특징으로 하는 상기 방법.

도면

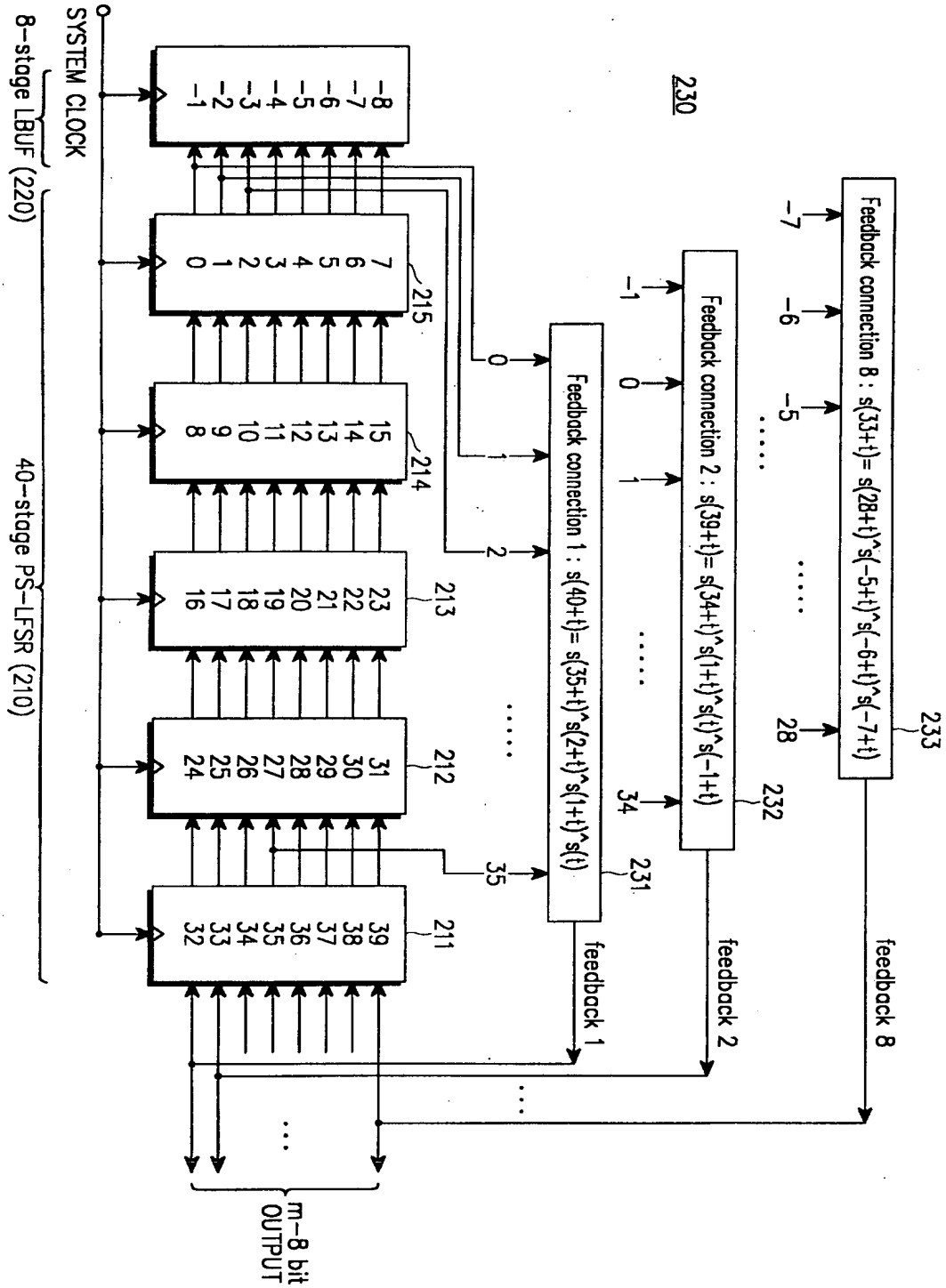
도면 1


SYSTEM CLOCK
0
1
2
3
4
5
.....
i
.....
n-1
n-stage LFSR
10
Feedback connection : the primitive connection
20
Output
1

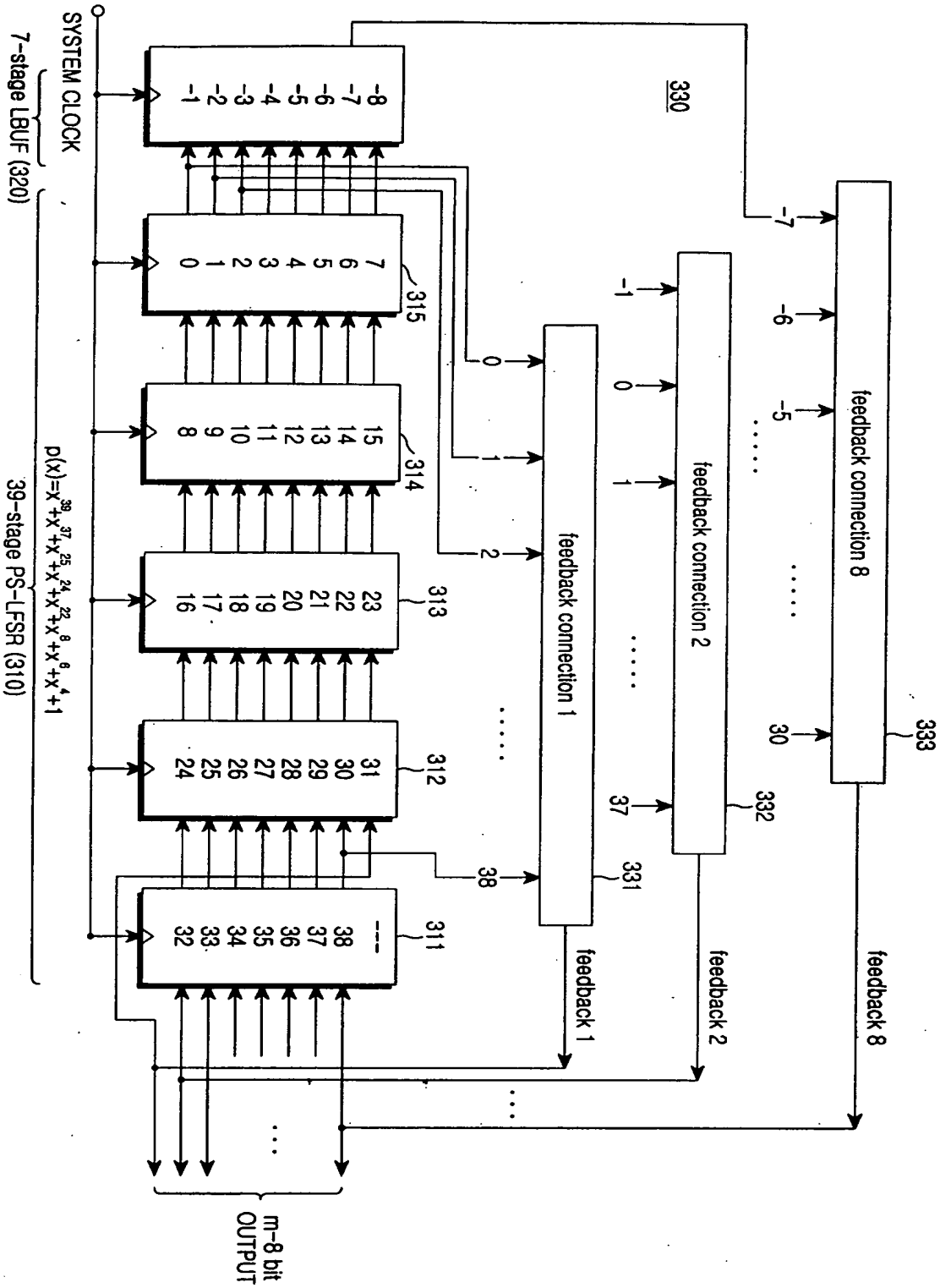
도면 2


130
Feedback connection m :m-bit left-shifting of the primitive combination
133
-(m-1) -(m-2) -(m-3)
n-m+1
Feedback connection 2 :1-bit left-shifting of the primitive combination
132
-1 0 1
n-2
Feedback connection 1 : the primitive combination
131
0 1 2
n-1
feedback m
feedback 2
feedback 1
-m
-(m-1)
-5 -4 -3 -2 -1
m-1
5 4 3 2 1 0
115
2m-1
m+5 m+4 m+3 m+2 m+1 m
114
3m-1
2m+5 2m+4 2m+3 2m+2 2m+1 2m
113
112
n-1
n-2 n-3 n-4 n-5 n-6
n-m
111
SYSTEM CLOCK
(m-1)-stage LBUF (120)
n-stage PS-LFSR (110)
m-bit
OUTPUT

도면 3


230
SYSTEM CLOCK
8-stage LBUF (220)
40-stage PS-LFSR (210)
Feedback connection 8 : s(33+t)= s(28+t)^s(-5+t)^s(-6+t)^s(-7+t)
Feedback connection 2 : s(39+t)= s(34+t)^s(1+t)^s(t)^s(-1+t)
Feedback connection 1 : s(40+t)= s(35+t)^s(2+t)^s(1+t)^s(t)
feedback 8
feedback 2
feedback 1
m-8 bit OUTPUT
233
232
231
211
212
213
214
215

도면 4


SYSTEM CLOCK
7-stage LBUF (320)
39-stage PS-LFSR (310)
p(x)=x^39+x^37+x^25+x^24+x^22+x^8+x^6+x^4+1
330
315
314
313
312
311
331
332
333
feedback connection 1
feedback connection 2
feedback connection 8
feedback 1
feedback 2
feedback 8
m-8 bit OUTPUT